国家互联网应急中心

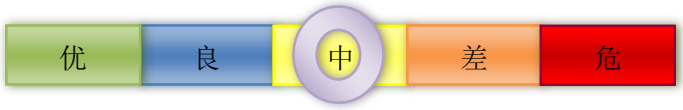
网络安全信息与动态周报

2020 年第 9 期

2 月 24 日-3 月 1 日

CNCERT/CC

本周网络安全基本态势

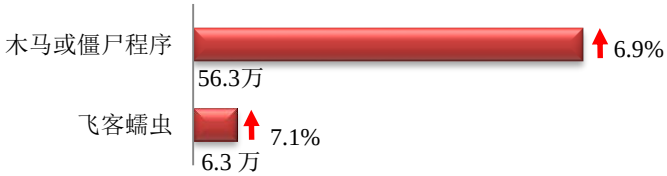


境内感染网络病毒的主机数量	•62.6万	↑ 7.1%
境内被篡改网站总数 其中政府网站数量	•9140 •45	↓ 5.1% ↓ 2.2%
境内被植入后门网站总数 其中政府网站数量	•1537 •1	↓ 12.0% ↓ 85.7%
针对境内网站的仿冒页面数量	•996	↑ 34.6%
新增信息安全漏洞数量 其中高危漏洞数量	•699 •288	↑ 36.0% ↑ 44.0%

= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少

本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 62.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 56.3 万以及境内感染飞客（conficker）蠕虫的主机约 6.3 万。



针对 CNCERT 自主监测发现以及各单位报送数据，CNCERT 积极协调域名注册机构等进行处理，同时通过 ANVA 在其官方网站上发布恶意地址黑名单。

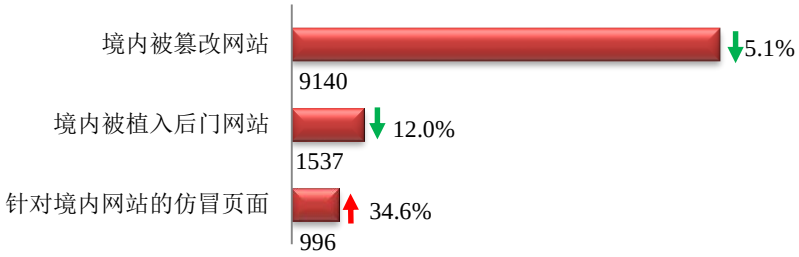
ANVA恶意地址黑名单发布地址

http://www.anva.org.cn/virusAddress/listBlack

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

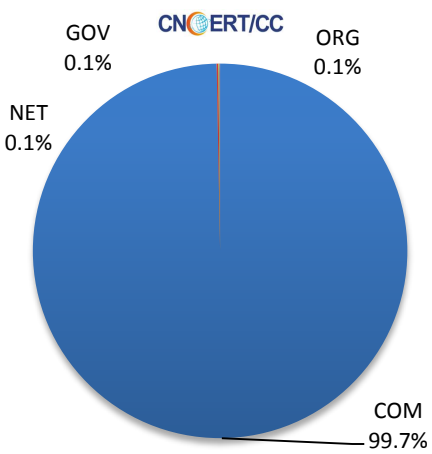
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 9140 个；被植入后门的网站数量为 1537 个；针对境内网站的仿冒页面数量 996 个。

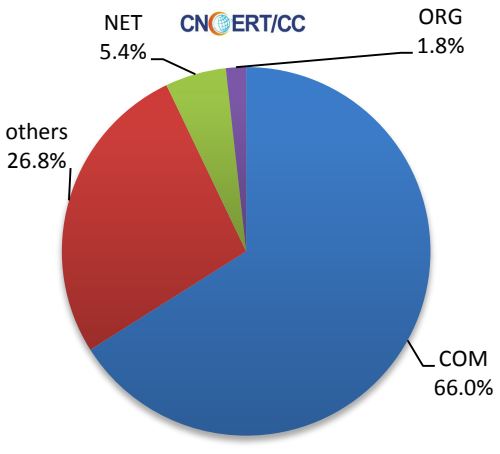


本周境内被篡改政府网站（GOV 类）数量为 45 个（约占境内 0.5%），较上周下降了 2.2%；境内被植入后门的政府网站（GOV 类）数量为 1 个（约占境内 0.1%），较上周下降了 85.7%。

本周我国境内篡改网站按类型分布
(2/24-3/1)

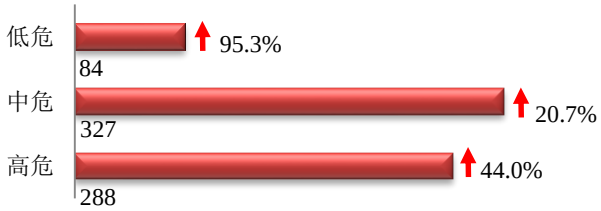


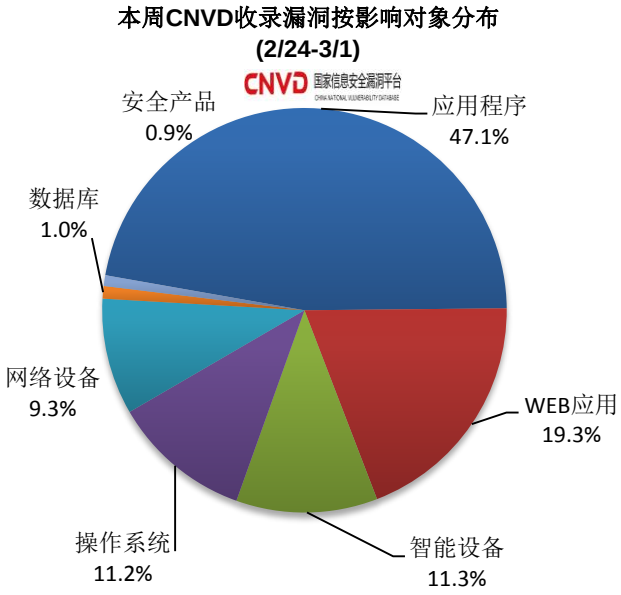
本周我国境内被植入后门网站按类型分布
(2/24-3/1)



本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 699 个，信息安全漏洞威胁整体评价级别为中。





本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是 WEB 应用和智能设备。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

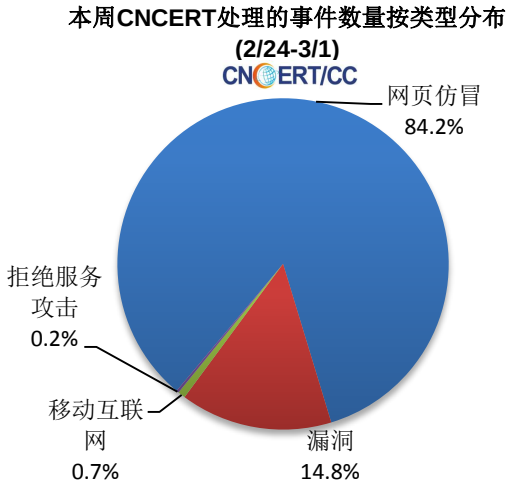
CNVD漏洞周报发布地址

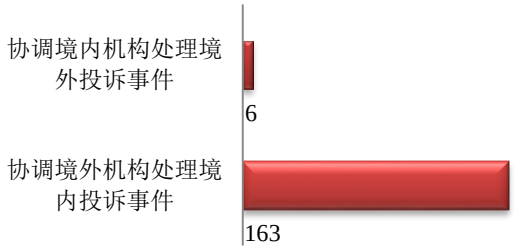
http://www.cnvd.org.cn/webinfo/list?type=4

国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

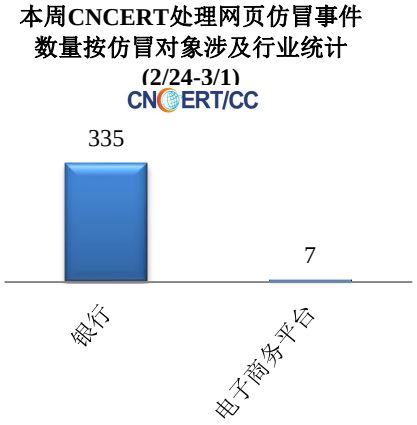
本周事件处理情况

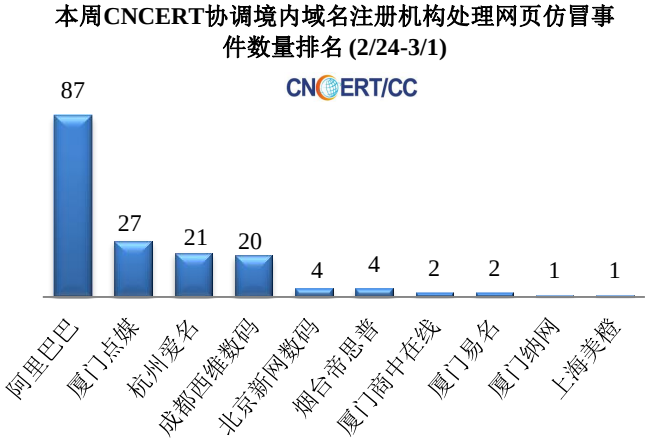
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 411 起，其中跨境网络安全事件 169 起。



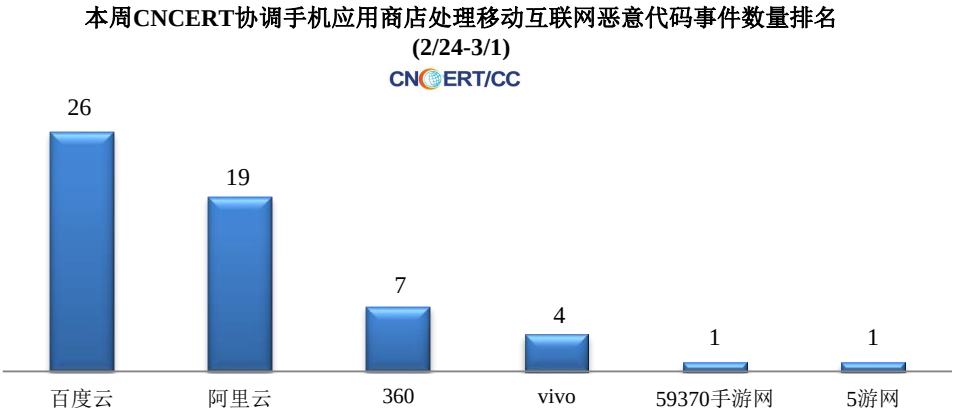


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 346 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 335 起和电子商务平台 7 起。





本周，CNCERT 协调 6 个应用商店及挂载恶意程序的域名开展移动互联网恶意代码处理工作，共处理传播移动互联网恶意代码的恶意 URL 链接 58 个。



业界新闻速递

1、 《网络信息内容生态治理规定》正式施行

2 月 29 日消息，从 3 月 1 日起，《网络信息内容生态治理规定》开始施行。规定明确，网络信息内容服务使用者和生产者、平台不得开展网络暴力、人肉搜索、深度伪造、流量造假、操纵账号等违法活动。网络信息内容生产者应当遵守法律法规，防范和抵制制作、复制、发布含有“使用夸张标题，内容与标题严重不符”和“炒作绯闻、丑闻、劣迹”等不良信息等。

2、 谷歌发现两个严重的零日漏洞

2 月 26 日，cnBeta 网消息，谷歌当日发布了一个 Chrome 更新程序，以修复三个安全漏洞。其中包括一个零日漏洞补丁，目前正在被利用。目前，有关这些攻击的详情尚未公开，不过有媒体指出，谷歌威胁分析团队成员于 2 月 18 日发现了这一问题。该团队作为谷歌下设的一个部门，其主要负责调查和追踪安全威胁的来源。谷歌已发布了面向针对多个操作系统的 Chrome 80.0.3987.122 更新，但 Chrome OS/iOS/Android 版本还未发布。

3、 Wi-Fi 漏洞 KrOOk 曝光 全球数十亿台设备受影响

2 月 26 日，外媒 ZDNet 消息，由赛普拉斯半导体和博通制造的 Wi-Fi 芯片存在严重安全漏洞，让全球数十亿台设备非常容易受到黑客的攻击，能让攻击者解密他周围空中传输的敏感数据。安全公司 ESET 在 RSA 会议上详细介绍了这个漏洞，黑客可以利用称为 Kr00k 的漏洞来中断和解密 Wi-Fi 网络流量。该漏洞存在于赛普拉斯和博通的 Wi-Fi 芯片中，而这是拥有全球市场份额较高的两大品牌，从笔记本电脑到智能手机、从 AP 到物联网设备中都有广泛使用。其中亚马逊的 Echo 和 Kindle、苹果的 iPhone 和 iPad、谷歌的 Pixel、三星的 Galaxy 系列、树莓派、小米、华硕、华为等品牌产品中都有使用。保守估计全球有十亿台设备受到该漏洞影响。

关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截至 2019 年，CNCERT 与 76 个国家和地区的 233 个组织建立了“CNCERT 国际合作伙伴”关系。

联系我们

如果您对 CNCERT《网络安全信息与动 态周报》有何意见或建议，欢迎与我们的编辑交流。

本期编辑：肖崇蕙

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315